UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,301	08/16/2001	Steven Black	AUS920010242US1	3154

35525 7590 01/24/2006

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,301	BLACK ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 21. Claims 1, 8 and 15 have been amended in an amendment filed on 12/13/2005. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 21.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 – 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Farley et al. (Publication Number: 2002/0078381), in view of Drake et al. (US Patent 6347374).

As per claim 1, 8 and 15, Drake teaches a method in a data processing system for reporting security situations, comprising the steps of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (Farley, see example, Para [0019] Line 1 – 3 and Para [0019] Line 12 – 17: SRC / DEST / EVENT TYPE as the event attribute parameters);

Farley teaches classifying and correlating the raw events (Farley, Para [0019] Line 1 – 3). However, Farley does not disclose expressly classifying events as groups by aggregating events with at least one attribute within the event set as an identical value.

Drake teaches classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (Drake, see example, Column 11 Line 38 – 50 and Column 14 Line 18 – 21: Drake teaches aggregating the correlated raw events into event groups with at least one attribute within the event set as an identical value such as (a) same user ID, or (b) same group type as "authentication failure" to generate an alert of severity situations).

calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group (Drake, see example, Column 12 Line 29 – 30, Column 11 Line 38 – 50 and Column 14 Line 18 – 21: the "authentication failure" is qualified to meet the severity level as an event caused by the failures of a user login).

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value (Drake, see example, Column 11 Line 38 – 50 and Column 14 Line 18 – 21: the "authentication failure" is qualified to meet the severity level as an event caused by the failures of a user login when the aggregating events exceed the predetermined number (i.e., threshold = 3) as taught by Drake).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Drake within the system of Farley because (a) Farley teaches classifying and correlating raw events by providing a security management system in a networked computer system (Farley, Para [0019] Line 1 – 3 and Para [0016]) and (b) Drake teaches improving network security by providing an effective event detecting systems (Drake, see example, Column 2 Line 4 – 8 and Column 3 Line 34 – 35).

As per claim 2, 9 and 16, Farley as modified further teaches the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups (Drake, see example, Column 11 Line 38 – 50 and Column 14 Line 18 – 21: Drake teaches aggregating the correlated raw events into event groups with at least one attribute within the event set as an identical value such as (a) same user ID, or (b) same group type as "authentication failure" to generate an alert of severity situations).

As per claim 3, 10 and 17, Farley as modified further teaches the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation (Farley: Para [0016] Line 1 – 10).

As per claim 4, 11 and 18, Farley as modified further teaches calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group (Burrows: Para [0050] Line 3 – 9: the "broadcast storm" is qualified to meet the severity level as an event caused by the identical SRC and different DEST when the aggregating events exceed the predetermined number (i.e., threshold) as taught by Burrows).

As per claim 5, 12 and 19, Farley as modified further teaches the target attribute represents one of a computer and a collection of computers (Farley, see example, Para [0019] Line 1 – 3 and Para [0019] Line 12 – 17: SRC / DEST / EVENT TYPE as the event attribute parameters).

As per claim 6, 13 and 20, Farley as modified further teaches further teaches the source attribute represents one of a computer and a collection of computers (Farley,

see example, Para [0019] Line 1 – 3 and Para [0019] Line 12 – 17: SRC / DEST / EVENT TYPE as the event attribute parameters).

As per claim 7, 14 and 21, Farley as modified further teaches aggregating a subset of the groups into a combined group (Farley, see example, Para [0079] and [0080]; Burrows, see example, Para [0050] and Para [0046] Line 10 – 11).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

Longbit Chai
Examiner
Art Unit 2131

Primary Examiner
AU 2131
1/21/06